REMARKS

The Applicants request reconsideration of the rejection.

Claims 1-8 and 18-27 are now pending, including new independent claim 27.

The Applicants have carefully considered the Examiner's Response to Arguments set forth on pages 2-4 of the Office Action. To focus the discussion on just a few disputed issues raised by the Examiner, the Applicants address only those comments that should be resolved at this time.

On page 3 of the Office Action, in discussing the Applicants' assertion that Jaffe discloses that "Operations are performed using a data representation such that the Hamming weight of all input values is constant," the Examiner nevertheless states that even though the values are operated on using a constant Hamming weight data representation, "at least the logic values that are initially input before the data is converted into the constant Hamming weight representation <u>do not necessarily have a constant Hamming weight</u>" (emphasis added). As a principle of basic logic, that Jaffe's logic values do not <u>necessarily</u> have a constant Hamming weight does not constitute a statement that Jaffe's logic values <u>do not have</u> a constant Hamming weight. Absent a <u>teaching</u>, the person of ordinary skill is not led from Jaffe, even taken in combination with the admitted prior art, to the invention set forth in claim 1. Indeed, as set forth in the sentence bridging pages 5-6 of the Office Action, the Examiner recognizes that the absence of a positive recitation in Jaffe's specification is not a basis for an exclusion (i.e., the negative limitation that the input data does not have a constant Hamming weight), but nevertheless makes that error. To find otherwise is to read claim 1 <u>into</u> Jaffe's specification, which is manifestly improper.

In addition, the sentence bridging pages 3-4 of the Office Action affirms that the admitted prior art is silent as to whether the input data has a constant Hamming weight, but asserts that there is “no limitation placed on some of the data in the system, namely the disturbance data.” Fundamentally, if the admitted prior art is silent as to whether the input data has a constant Hamming weight, and if the secondary reference to Jaffe is also silent as to whether the input data has a constant Hamming weight, the combination of these two references fails to teach input data having a non-constant Hamming weight. In addition, the Applicants fail to see the relevance of the argument that “there is no limitation placed on some of the data in the system, namely the disturbance data.” That there may be no limitation placed on some of the data does not provide the teaching missing as above. Further, the disturbance data has a constant Hamming weight, according to claim 1 (and new claim 27).

Turning to the objections and rejections, the Examiner objected to the specification for failing to provide proper antecedent basis for the limitation “wherein said input data D1 does not have a constant Hamming weight” in claim 1. However, the Applicants respectfully submit that it is self-evident that the input data D1 does not have a constant Hamming weight.

It is a precondition that the transformed data from the input by using disturbance data has the same representation as the input data. That is, the number of bits or the bit length is not changed or transformed. The input data can employ any combination of 0’s and 1’s in the number of bits or the bit length. Tthese combinations include a case where the bits are either all 0’s or all 1’s. Further, a Hamming weight of 0 is the Hamming weight of data having only 0’s. Therefore, among all of the combination of 0's and 1's, there are at least a case of a 0 Hamming weight and a case of a Hamming weight that is non-zero, so that the Hamming weight is not constant in the transformation.

Backing up a bit, the "Hamming weight of data" is the number of bits each having a logic value of 1 in the binary representation of the data. For example, in an embodiment implementing a technique for transmitting a Ptext (plain text) 3201, as discussed on page 69 of the present specification, "the Ptext plain text 3201 is transformed by using PX plaint-text disturbance data 3203 in a first transformed process 3202 to produce Xptext transformed plain text 3204." Continuing, "the Xptext transformed plain text 3204 is subjected to IP permutation 3205 for generating 32 high-order bits and 32 low-order bits." This flow is the same as the "data flow of the ordinary DES encryption." Data of 32 bits is transformed into the same representation of 32 bits. The representation of 32 bits employs all combination of 2^{32}. Thus, as stated above, among all of the combinations of 0's and 1's, there are at least a case of Hamming weight of 0, and a case of Hamming weight of non-zero, so that the Hamming weight is not constant. The ordinary DES description is the "DATA ENCRYPTION STANDARD (DES)" which is well known to the person of ordinary skill in the art. For the record, a copy of the specification of DES is enclosed with this paper.

Of course, the claimed embodiments are not all limited by having input data having a constant Hamming weight. It is simply claim 1 (and its dependent claims) that are limited by input data having a non-constant Hamming weight, according to the Applicants' decision. Other claims, including new independent claim 27, are not so limited.

In summary, the limitation of claim 1 “wherein said input data D1 does not have a constant Hamming weight” is fully supported by the present specification when taken in consideration with the knowledge of the person of ordinary skill in the art. That is, the analysis set forth above, taken directly from the specification, leads to the conclusion that the disclosed embodiment, claimed in claim 1, has input data of a non-constant Hamming weight. Accordingly, the Applicants request reconsideration of the rejection.

Claims 18-22 stand rejected under 35 U.S.C. §112, second paragraph, as being indefinite for the antecedent basis problem set forth on page 6 of the Office Action. This rejection is overcome by the amendment above.

Turning to the prior art rejections, claims 23, 25 and 26 were rejected under 35 U.S.C. §102(a) as being anticipated by the Applicants’ admitted prior art. The subject matter of claim 23 has been added to claim 24, and the dependency of claims 25 and 26 changed to claim 24. Therefore, this rejection is moot. The Applicants make no admission as to the propriety of the rejection.

Claims 18 and 20-22 stand rejected under 35 U.S.C. §103(a) as being unpatentable over the admitted prior art. The subject matter of claim 19 has been added to claim 18. Therefore, this rejection is also moot. The Applicants do not admit to the propriety of the rejection.

Claims 1-8, 19 and 24 stand rejected under 35 U.S.C. §103(a) as being unpatentable over the admitted prior art in view of Jaffe et al., U.S. Patent No. 6,510,518 (Jaffe). In response to the Applicants’ previous argument that Jaffe does not disclose input data having a non-constant Hamming weight, the present rejection asserts that this feature is found in the admitted prior art. However, the rejection refers to page 21 of the present application, which makes no reference to the Hamming weight of the input data. Therefore, even in combination with Jaffe, there is no *prima facie* case of obviousness of claims 1-8 because Jaffe teaches away from the limitation by requiring a constant Hamming weight representation.

However, even if the admitted prior art or Jaffe were to employ input data not having a constant Hamming weight, the present claim 1 has additional patentability in requiring disturbance data that possesses a constant Hamming weight. That is, even if one considers Jaffe to provide input data having a non-constant Hamming weight, the transforming of the data is different between the present invention and Jaffe.

As noted above, Jaffe uses a constant Hamming weight representation, so realizing tamper resistance. Jaffe, however, does not use disturbance data itself that corresponds to the disturbance data set forth in the present claims. Therefore, Jaffe provides no motivation for modifying the admitted prior art to use the claimed disturbance data.

Moreover, the admitted prior art does not teach the disturbance data employed as set forth in claim 1. The admitted prior art teaches that, in order to improve tamper resistance, data to be processed is first transformed by using data for disturbance, so that the degree of correlation between the magnitude of a current consumed during the processing and the original data is lowered. The transformed data is then processed. Finally, a result of the processing is subjected to inverse transformation by using the disturbance data or by using a result of processing the disturbance data to produce a value equal to data which will be obtained as a result of processing the original data.

However, there is no suggestion in the admitted prior art to make constant the Hamming weight for the disturbance data. Therefore, merely combining the admitted prior art with Jaffe does not lead the person of ordinary skill to the presently claimed invention.

Even page 21, lines 1-12 (cited in the present Office Action) do not support the allegation underlying the rejection. According to this passage, "in the prior technology, however, there is no limitation imposed on the data for disturbance. Thus, by monitoring a current consumed during processing of the data for disturbance, the data for disturbance can be inferred. Then, by classifying the inferred data, the attack cited before can be launched." That "there is no limitation placed in the disturbance data" does not provide the necessary teaching that the disturbance data has a constant Hamming weight.

Therefore, in view of the foregoing arguments, the invention claimed in claims 1-8 cannot be said to be rendered obvious by any combination of the admitted prior art and Jaffe.

As regards claims 18 and 24 (claim 18 being amended to include the subject matter of claim 19), a feature of these claims is that the appearance probabilities of the logic value 0 or 1 at each position of the first disturbance data and the second data disturbance data are set at 50%. By this feature, the Hamming weight is approximately constant. Therefore, in accordance with the foregoing argument emphasizing the lack of prior art teaching with respect to disturbance data having a constant Hamming weight, claims 18 and 24 are also patentable.

Dependent claims 2-8 inherit the patentable features of independent claim 1 from which they are derived. Accordingly, for brevity, the separate patentability of these claims will not be argued at this time. The Applicants make no admission as to the propriety of the rejection.

In view of the foregoing amendments and remarks, the Applicants request reconsideration of the rejection and allowance of the claims.

To the extent necessary, the Applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the deposit account of Mattingly, Stanger, Malur & Brundidge, P.C., Deposit Account No. 50-1417 (referencing attorney docket no. NIT-295).

Respectfully submitted,

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.

/Daniel J. Stanger/
Daniel J. Stanger
Registration No. 32,846

DJS/sdb
(703) 684-1120